

METHOD FOR APPLYING COMPETENCE BY USING LICENSE

Publication number: JP2001255953 (A)

Publication date: 2001-09-21

Inventor(s): SCHMIDT ERNST; KUHLS BURKHARD +

Applicant(s): BAYERISCHE MOTOREN WERKE AG +

Classification:

- **international:** B60R25/00; G06F12/14; G06F21/22; G06F21/24; G09C1/00; B60R25/00; G06F12/14; G06F21/00; G06F21/22; G09C1/00;

(IPC1-7): G06F1/00; G06F12/14; G09C1/00

- **European:** B60R25/00

Application number: JP20010032508 20010208

Priority number(s): DE20001008973 20000225

Also published as:

EP1127756 (A2)

EP1127756 (A3)

EP1127756 (B1)

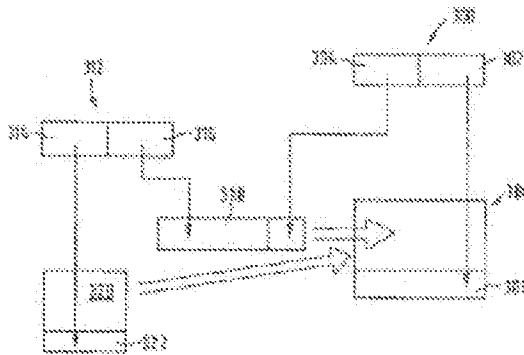
US2002023223 (A1)

US7197637 (B2)

[more >>](#)

Abstract of JP 2001255953 (A)

PROBLEM TO BE SOLVED: To provide a method for guaranteeing the data maintainability of software for the controller of an automobile. **SOLUTION:** A pair of controller keys 300, having first and second keys and the prescribed number n of license key pairs 312 having the first and second keys, are used. The license information of the first license 318 is signed by using the second key 304 of the controller key pair 300, and software (320) to be newly inputted to a controller 360 is signed 322 by using the second key 314 in the license key pair 312, in which the first key is arranged in the license information of the last license.



.....
Data supplied from the **espacenet** database — Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-255953

(P2001-255953A)

(43)公開日 平成13年9月21日 (2001.9.21)

(51)Int.Cl. ⁷	識別記号	F I	マーク(参考)
G 0 6 F 1/00 12/14	3 2 0	C 0 6 F 12/14	3 2 0 A
G 0 9 C 1/00	6 4 0	C 0 9 C 1/00	6 4 0 B
		C 0 6 F 9/06	6 6 0 C

審査請求 未請求 請求項の数19 O L (全 12 頁)

(21)出願番号	特願2001-32508(P2001-32508)
(22)出願日	平成13年2月8日 (2001.2.8)
(31)優先権主張番号	1 0 0 0 8 9 7 3 : 9
(32)優先日	平成12年2月25日 (2000.2.25)
(33)優先権主張国	ドイツ (DE)

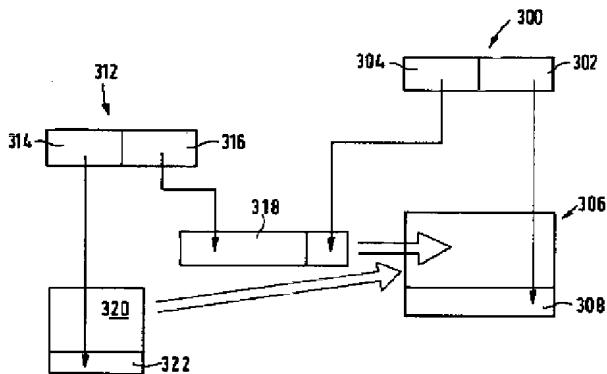
(71)出願人	391009671 バイエリッシェ モートーレン ウエルケ アクチエンゲゼルシャフト BAYERISCHE MOTOREN WERKE AKTIENGESELLS CHAFT ドイツ連邦共和国 テー・80788 ミュン ヘン ベツエルリング 130
(74)代理人	100063130 弁理士 伊藤 武久 (外1名)

最終頁に続く

(54)【発明の名称】 認可証を用いて権限を与える方法

(57)【要約】

【課題】 自動車両の制御装置用のソフトウェアのデータ保全性を保証するための方法を提供する。
【解決手段】 第1鍵と第2鍵を有する制御装置鍵ペア (300) と、第1鍵と第2鍵をそれぞれに有する所定数nの認可証鍵ペア (312) を使用する。第1認可証 (318) の認可証情報は、制御装置鍵ペア (300) の第2鍵 (304) を用いて署名され、制御装置 (306) に新たに投入すべきソフトウェア (320) は、第1鍵が最後の認可証の認可証情報内に整理されている認可証鍵ペア (312) における第2鍵 (314) を用いて署名 (322) される。



【特許請求の範囲】

【請求項1】自動車両の制御装置のためのソフトウェアのデータ保全性を保証するための方法であって、作動方式に関して制御装置に影響を及ぼすソフトウェアがメモリ内に記憶され得る前記方法において、以下のステップを含むことを特徴とする方法：第1鍵と第2鍵を有する制御装置鍵ペアを提供するステップ。第1鍵と第2鍵をそれぞれに有する所定数nの認可証鍵ペアを提供するステップ。制御装置鍵ペアの第1鍵を自動車両内の制御装置内または自動車両内の制御装置のために保管するステップ。所定数nに対応する認可証を作成するステップ。この際、各認可証は認可証情報を含み、最後の認可証の認可証情報内にはソフトウェアをチェックするための少なくとも1つの鍵が整理されていて、並びに、複数の認可証を使用する場合、他の認可証情報内には次に続く認可証をチェックするための少なくとも1つの鍵が整理されていること。制御装置鍵ペアの第2鍵を用いて第1認可証の認可証情報を署名するステップ、並びに、認可証が1つよりも多い場合には、前の認可証の認可証情報内にそれぞれの第1鍵が整理されている認可証鍵ペアにおけるそれぞれの第2鍵を用いて、次に続く認可証を署名するステップ。最後の認可証の認可証情報内に第1鍵が整理されている認可証鍵ペアにおける第2鍵を用いて、新たに投入すべきソフトウェアを署名するステップ。署名された全ての認可証を制御装置内に投入するステップ。署名されたソフトウェアを制御装置内に投入するステップ。制御装置内または制御装置のために保管されている制御装置鍵ペアの第1鍵を用いて第1認可証の署名をチェックするステップ、並びに、認可証が1つよりも多い場合には、前の認可証の認可証情報内に含まれている第1鍵を用いて他の各認可証の署名をチェックするステップ。それぞれのチェックが肯定的な結果を導く場合に、それぞれの認可証の認可証情報を受諾するステップ。最後の認可証の認可証情報内に保管されている第1鍵を用いてソフトウェアの署名をチェックするステップ。及び、このチェックも肯定的な結果を導く場合に、投入されているソフトウェアを受諾するステップ。

【請求項2】認可証内に少なくとも1つの認可証情報をとして公開鍵を含むこと、及び、この公開鍵を用いてチェックすべき署名を付属の秘密鍵を用いて実施することを特徴とする、請求項1に記載の方法。

【請求項3】制御装置内または制御装置のために保管されている制御装置鍵ペアの第1鍵が公開鍵であること、及び、付属の秘密鍵を用いて、第1認可証の署名を実施することを特徴とする、請求項1または2に記載の方法。

【請求項4】車両、特に車両内の制御装置が、公開鍵と秘密鍵を有する非共通性の一対の鍵を生成すること、車両内、特に制御装置内に前記秘密鍵を保管すること、及

び、第1認可証を署名するために前記公開鍵を車両から読み出し可能とすることを特徴とする、請求項1または2に記載の方法。

【請求項5】制御装置内に保管される鍵を制御装置のポートセクタに整理することを特徴とする、請求項1～4のいずれか一項に記載の方法。

【請求項6】ポートセクタを、書き込み及び鍵の入力の後にロックし、他のアクセス、特に書き込みアクセスに対して保護することを特徴とする、請求項5に記載の方法。

【請求項7】ソフトウェア及び／または認可証情報を所定の長さを有する情報にそれぞれ写像し、これらの情報を署名することを特徴とする、請求項1～6のいずれか一項に記載の方法。

【請求項8】写像機能としてハッシュ機能を選択することを特徴とする、請求項7に記載の方法。

【請求項9】制御装置を含む車両の少なくとも1つの車両固有情報をソフトウェアに付加すること、ソフトウェアと共に少なくとも1つの前記車両固有情報を署名すること、認可証の署名のチェックとソフトウェアの署名のチェックに加えて前記車両固有情報もチェックすること、及び、更にソフトウェアの前記車両固有情報が車両の車両固有情報と一致する場合にだけ制御装置内にてソフトウェアを受諾することを特徴とする、請求項1～8のいずれか一項に記載の方法。

【請求項10】車両固有情報をチェックするために固有の車両固有鍵ペアを生成し、車両固有情報及び前記車両固有鍵ペアの1つの鍵を車両安全ユニット内または制御装置内に設け、車両固有情報に加えて前記車両固有鍵ペアの他の鍵をソフトウェア内に整理し、投入されているソフトウェアの受諾の同意のために、前記車両固有鍵ペアの両方の鍵が互いに調和しているかどうかを別個のルーチンでチェックすることを特徴とする、請求項9に記載の方法。

【請求項11】少なくとも制御装置の最初の立ち上げ時にソフトウェアを検査し、更に対応してマーキングすることを特徴とする、請求項1～10のいずれか一項に記載の方法。

【請求項12】制御装置に外部からアクセスする際に、アクセスのための資格があるかどうかをアクセスユニットが検査することを特徴とする、請求項1～11のいずれか一項に記載の方法。

【請求項13】制御装置からのコードを要求し、このコードの正確性について検査することを特徴とする、請求項12に記載の方法。

【請求項14】制御装置が乱数を発信し、この乱数をアクセス側が署名すること、及び、この署名を制御装置内、特に確認鍵を用いてチェックすることを特徴とする、請求項13に記載の方法。

【請求項15】アクセス資格の試問時に資格レベルを決

定し、この資格レベルに依存してアクセス行為を受諾または非受諾とすることを特徴とする、請求項12～14のいずれか一項に記載の方法。

【請求項16】車両内の安全装置が、少なくとも散発的に制御装置の信頼性検査を実施し、否定的な結果の場合にはその制御装置を記録することを特徴とする、請求項1～15のいずれか一項に記載の方法。

【請求項17】制御装置内に制御装置固有の秘密コードを保管することを特徴とする、請求項16に記載の方法。

【請求項18】安全装置が、制御装置に特有の特徴を試問し、この特徴を信頼性に関して検査することを特徴とする、請求項16または17に記載の方法。

【請求項19】信頼性検査時に、安全装置内及び／または制御装置内に保管されている鍵を使用することを特徴とする、請求項16～18のいずれか一項に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、自動車両の制御装置のためのソフトウェアのデータ保全性を保証するための方法に関する。

【0002】

【従来の技術】車両内の電子装置、並びに車両との通信可能性が増加することにより、その安全性に対する要求も高まることになる。

【0003】車両の極めて異なる領域には制御用のマイクロコントローラが組み込まれている。これらの制御装置は今日では頻繁に1つのバスシステムまたは複数のバスシステムを介して互いに接続されている。更に、前記バスに外部からアクセスし、個々の制御装置と通信する極めて多くの可能性（例えば診断接続）が提供されている。

【0004】制御装置の機能方式はソフトウェアプログラムにより決定される。従来、制御装置（即ちコントローラ）内に組み込まれているソフトウェアは、多くの場合、プログラミング不可能なメモリ内（例えば、マスクプログラミングされているマイクロコントローラ）に整理（ファイル）されている。それにより、ソフトウェアの改ざんは簡単には実現され得ない。例えば、メモリ構成要素と他のメモリ構成要素との完全な交換は認識され、それに対応した反応が成され得る。

【0005】プログラミング可能、特に所謂フラッシュプログラミング可能な制御装置を将来的に車両にて使用することにより、資格を伴わない改ざんがソフトウェア並びにそれと共に制御装置の作動方式に施されるという危険性が増加する。つまり、権限をもたない人物により、手間のかからない新たなプログラミングによって簡単にソフトウェアの交換が実行されてしまう。

【0006】安全上の理由から、並びに法的な要求を満

たすためには、オリジナルソフトウェアの変更が防止されるか、またはその種の変更が権限をもつ人物にだけ認められるという措置がとられなければならない。

【0007】また、様々なモデルにて同じハードウェアを使用するという同部材コンセプトに注目することは将来的に有利であろう。そうすれば、機能方式における差異は、異なるソフトウェア内だけに留まることになる。このコンセプトにより、所定のソフトウェアは、固有の車両においてだけ実行可能であり、簡単に複写することは不可能となる。

【0008】従来の技術から、多数の確認方法（認証方法）並びに確認装置（認証装置）が知られている。

【0009】米国特許第5844986号明細書(US5844986)では、PCのBIOSシステムへの許可されない侵入を回避するために使用される方法について記載されている。BIOSメモリを含む暗号プロセッサが、公開鍵と秘密鍵を用いる所謂公開鍵方式（パブリックキー方式）をベースにしてBIOS変更の確認並びにチェックを実施する。この場合、前記チェックは、投入すべきソフトウェア内に埋め込まれているデジタル署名を検査することにより行われる。

【0010】EPO特許出願公開第0816970号明細書(EP0816970A2)からは、ファームウェアをチェックするための装置が知られている。ブート PROMメモリを確認するための前記装置は、マイクロコードを有するメモリ部分を含む。確認セクタは、マイクロコードの実施に対する回答としてハッシュデータを生成するハッシュジェネレータを含む。

【0011】しかし、上述の方法または装置では、自動車両の制御装置内に投入すべきソフトウェアを直接的にチェックすることはできない。

【0012】EPO特許出願公開第0813132号明細書(EP0813132A2)では、認可証及びアクセリストとプログラムを接続することが記載されている。その有利な実施形態に従い、認可証エージェンシーはコード用の認可証とアクセリスト用の認可証を作成する。認可証が一度授与されると、認可証を侵害することなくコードまたはアクセリストを変更することは不可能である。コードとアクセリストは、それらの認可証と共にサーバ内にて記憶される。この方法を用いて、コードまたはアクセリストを要求する顧客は、それらの信頼性を確認することができる。しかし、この方法を自動車両領域内にて使用することは簡単には可能ではない。

【0013】通常、要求されているソフトウェアの提供、並びにその真正な特徴付け（マーキング）のために複数の有資格者が起用されることは有利である。それにより、特徴付けは中央箇所だけで行われる必要はない。無論、選択されている有資格者のために、資格を授与するための中央監視箇所が更に設置されるべきである。

【0014】

【発明が解決しようとする課題】本発明の課題は、自動車両の制御装置用のソフトウェアのデータ保全性を保証するための方法を提供することにあり、この際、中央装置により管理可能である複数の有資格者は、真正なソフトウェアを提供し、対応して特徴付けることが可能である。

【0015】

【課題を解決するための手段】前記課題は、請求項1に記載した特徴により解決される。

【0016】それに従い、以下の記載ではトラストセンタと称する中央装置が有資格者に1つの認可証または複数の認可証を授与し得て、前記認可証を用いて、提供者（認可証所有者）は、制御装置自体のためのソフトウェアを正しく署名し且つ実行可能に車両内に投入することができる。

【0017】この目的のために、例えばトラストセンタ（選択的な実施形態では車両自体）が第1鍵と第2鍵を有する制御装置鍵ペア（制御装置用の一対の鍵）を提供する。第1鍵は、車両の製造時に制御装置自体に整理、または制御装置のために保管される。それが原因で、この一対の鍵は制御装置鍵ペアと称される。トラストセンタの第2鍵を用いて、第1認可証が、以下の記載では認可証所有者と記す有資格者のために署名される。

【0018】より明確にするために、先ずは、制御装置への新たなソフトウェアの実行可能な読み込みのために1つの認可証だけが必要とされる場合を仮定する。この1つの認可証は、認可証情報部分にて、所定の認可証情報の他に少なくとも認可証所有者の第1鍵を含み、ここで、第1鍵と第2鍵を有する認可証鍵ペア（認可証用の一対の鍵）は前記認可証所有者自身により生成されたものである。他の認可証情報としては、例えば、認可証発行者、通し番号、認可証所有者、所定のアクセス権利、有効期限などが確定され得る。

【0019】更に、有資格者または認可証所有者は、認可証鍵ペアの自らの第2鍵を用いて、制御装置内に投入すべきソフトウェアを署名する。認可証も、認可証所有者により署名されたソフトウェアも、引き続き車両の制御装置に投入される。制御装置は、制御装置鍵ペアの自らの固有の第1鍵を用いて認可証の正当性を認識し、認可証情報を受諾し、その中にはこの認可証情報内に含まれている鍵も含まれる。この鍵、即ち認可証鍵ペアの第1鍵を用いて、投入されているソフトウェアの署名のチェックが更に行われる。この署名も正しいと認識されると、前記ソフトウェアは制御装置により受諾される。

【0020】このプロセス方式により、変更権利及び署名権利が全般的に与えられる。各ソフトウェアは、制御装置鍵ペアの所有者自身、例えばトラストセンタ自身により署名される必要はない。それに加えて、認可証内の追加情報を用いて、認可証所有者に容認または制限を割り当てることが可能である。例えば、期間が容認され、

この期間に渡って認可証所有者はソフトウェアを提供し且つ投入することができる。ソフトウェアを生成するため及びソフトウェアの種類のための様々な資格レベルを授与することも可能である。ソフトウェア自体を署名することは、常に認可証所有者自身により行われる。

【0021】鍵としては、通常、周知の暗号アルゴリズムに使用されるコード化パラメータ及び／またはデコード化パラメータ（即ち、コード化パラメータ、またはデコード化パラメータ、またはコード化パラメータ及びデコード化パラメータ）として理解される。この際、対称方式並びに非対称方式の使用が可能である。対称方式では2つの鍵が同一であるので、実際には1つの鍵だけが異なる場所に設けられていることになる。非対称方式では異なる鍵が使用される。非対称方式としては、通常、公開鍵方式（パブリックキー方式）が知られていて、この公開鍵方式では公開鍵と秘密鍵（プライベート鍵）が生成される。公開鍵は誰にでも知られてよい。この種の非対称方式に関する暗号アルゴリズムは、例えば、リベスト(Rivest)、シャミール(Shamir)、エイドルマン(Adleman)によるRSAアルゴリズム、データ暗号アルゴリズム（DEAアルゴリズム）等のアルゴリズムである。これらのアルゴリズムは、第1鍵ペア（第1の一対の鍵）のためにも、第2鍵ペア（第2の一対の鍵）のためにも使用され得る。

【0022】本発明による方法の総合的な構成では、制御装置内に投入されるソフトウェアをチェックするために、唯一の認可証だけではなく複数の認可証nが与えられる。それにより、他の構成可能性も生じる。更に、異なる認可証を異なる人物に割り当てることが可能があるので、制御装置内への新たなソフトウェアの実行可能な投入は連帶してのみ可能となる。更に、異なる認可証数に渡って異なるアクセス権利を授与すること、即ち異なる認可証所有者に異なるアクセス権利を授与することが可能である。

【0023】複数の認可証の使用において、第1認可証の署名は、制御装置内に保管されている鍵を用いて検査され得る。それに対して他の各認可証の署名は、以前に受諾された認可証に含まれている鍵によりチェックされ得る。それに対して最後の認可証内の鍵を用いては、ソフトウェア自体の署名だけがチェックされる。全チェックが成功して経過した場合にだけ、ソフトウェアが制御装置により受諾される。認可証の署名を以前の認可証に含まれる鍵を用いてチェック可能とするために、認可証は前記鍵に付属する第2鍵を用いて署名されたものでなくてはならない。

【0024】秘密鍵及び公開鍵をそれぞれ何処に整理すべきかという選択では多くのバリエーションの可能性がある。例えば、公開鍵は認可証の認可証情報内にそれぞれ整理されている。制御装置自体内にも、制御装置鍵ペアの公開鍵が整理され得る。この場合、チェックすべき

署名は、公開鍵に付属する秘密鍵を用いて形成されたものである必要がある。

【0025】当然のことながら他の実施形態も考慮することができ、それでは、認可証情報内及び／または制御装置自体内に秘密鍵が保管されている。また、対称鍵との組合せも考えることができる。

【0026】制御装置内に保管されている鍵は有利にはブートセクタ内に整理されている。ブートセクタは、通常、特有の方式で保護されている。安全性の向上のために、このブートセクタは、書き込み及びこのブートセクタ内に含まれる鍵の整理の後に「ロック」される、即ち将来的なアクセス、特に書き込みアクセスが禁止されるようにもブートセクタは形成され得る。

【0027】全検査（認可証検査とソフトウェア検査）が肯定的な結果を示すと、ソフトウェアは、制御装置により、またはソフトウェアのために固有に設けられている装置により受諾され、制御装置の制御のために用いられる。

【0028】既に上述したように、所謂公開鍵方式における公開鍵は公開して周知としてよく、それに対して、秘密鍵は権限のある箇所においてだけ知られている。

【0029】実施形態に従い、制御装置鍵ペアの秘密鍵はトラストセンタにだけ、認可証鍵ペアの秘密鍵は認可証所有者にだけ知られている。秘密鍵を用いて、手書きのサインに対応して、デジタル署名が電子文書（認可証、ソフトウェア）に対して生成される。秘密鍵の所有者だけがその都度有効な署名を作成することができる。文書（認可証、ソフトウェア）の真実性は、公開鍵を用いた署名の検証を介してチェックされ得る。秘密鍵を知らない権限の無い第三者は、有効な署名を作成することはできない。改ざんされた認可証、または期限切れの認可証、または無資格の認可証が制御装置内にロードされた場合、または改ざんされていて且つ正しくなく署名されたソフトウェアが制御装置内にロードされた場合、このことはそれに付属の鍵を用いて認識され、制御装置は実行不可能な状態に置き換えられる。

【0030】対称方式の使用において、安全レベルを向上するためには、特有なハードウェアの形式の追加的な解決保護策が使用され得る。

【0031】ソフトウェアを独占的に車両固有に使用するという要求を可能とするためには、所定の車両の制御装置のために設けられているソフトウェアが、車両を個別化する情報、例えば車体番号または他の車両固有データを含む。これらの情報は、ソフトウェアに割り当て、またはソフトウェアに組み込まれている。これらのデータのソフトウェアへの割り当て、またはこれらのデータのソフトウェアへの組み込みの後に初めて、このソフトウェアは、最後の認可証の認可証所有者の第2鍵を用いて署名される。制御装置は、上述したように、一方では認可証が正しいと認識され、それに加えてソフトウェア

の署名が正しいと認識される場合にだけソフトウェアを受諾する。署名は、ソフトウェアに含まれている車両固有情報に依存するので、後から追加的に変更され得ない。車両固有情報が変更されていないと車両の車両固有情報と一致する場合には、ソフトウェアだけが車両の制御装置のために実行可能に入力され得る。それにより、この種の個別化されているソフトウェアを他の車両に複写することは不可能である。

【0032】更に、制御装置のメモリにソフトウェアを投入する際に他の安全レベルを提供するために、ソフトウェアの投入以前に、制御装置のメモリに対するアクセスは対応する資格を用いてのみ可能となるべきである。そのために、署名されているソフトウェアの移行以前に、申告ステップ内にて制御装置の「アンロック」が設けられている。申告時に様々な優先レベルを使用する場合、それにより、異なって形成されているアクセス権利が与えられ得る。診断アクセス時には、例えば先ず申告が必要不可欠であり、それにより制御装置は入力されたアクセス情報を介してアクセス権利、並びにこのアクセス権利と結び付けられている資格レベルを認識する。権利授与に応じて、アクセス資格は厳しくないものから極めて厳しいものまでレベル付けされ得る。権利授与は静的に形成され得るので、例えば、異なるアクセスコードが所定の資格レベルのために伝達される。選択的に権利授与は動的にも形成され得るので、例えば、認可証情報内に資格レベルを含むエントリ認可証が与えられる。

【0033】1つの選択として、署名のチェックは制御装置自体内にて実施される。他の選択として、少なくともチェックはエントリ制御装置ないしはアクセス制御装置内にてチェックされ得る。場合によってはアクセス制御のためだけに設けられている制御装置は、他の制御装置に比べて、アクセス権利の授与に関する中央安全機能があるために、アクセスできないように車両内に設けられている。これは、制御装置の物理的な解体により上述の保護機構が場合によってはすり抜けられてしまうためである。

【0034】更に、制御装置が完全に解体され、他の制御装置と取り替えられる危険性を排除するために、追加的な制御装置解体防止策を設けることは有意義である。この目的のために、例えば、制御装置が組み込まれている車両内で、散発的に制御装置信頼性検査が実施される。このためには、照会が各制御装置に向けて時折発せられ、これらの制御装置はその照会に対して所定の期待情報を用いて回答しなくてはならない。実際にチェックすべき制御装置からの発信情報が期待情報と一致しない場合、または制御装置が回答しない場合には、適切な保護措置がとられ、例えば、制御装置を通信接続から除外する、または制御装置を記録、マーク、またはリストに登録するなどである。それにより、車両の診断時には、ごまかし操作が認識され得る。上述の実施形態におい

て、制御装置は照会に対して例えば制御装置特有の秘密確認鍵を用いて回答する。不法に交換された制御装置は、その種の鍵を使用することができず、それにより受諾も成されない。

【0035】

【発明の実施の形態】次に、添付の図面を用いて実施形態に基づき本発明を更に詳細に説明する。

【0036】図1には、互いにネットワーク接続されているユニットを有する制御装置構成がブロック図として図示されている。この際、搭載ネットワークは、部分的に異なる伝送速度を有し且つ所謂ゲートウェイ（中央ゲートウェイモジュール、コントローラゲートウェイ）により互いに接続されている複数の部分ネットワーク（LWL-MOST（光導波路-MOST(Medi Oriental Systems Transport)）、K-CANシステム（カロッセリ（車体）-コントローラエリアネットワークーシステム）、パワートレーン-CAN等）から構成されている。診断バス16は中央ゲートウェイ14を用いて他の全てのネットワークと間接的または直接的に接続されている。この診断バス16は周囲環境への最も重要な接続部の1つである。この診断バス16の端部におけるOBDソケット(On Board Diagnose ソケット)に接続されている診断テストを介して、並びに中央ゲートウェイ14を介在して、全システム内の全てのコントローラ、ゲートウェイ、及び制御装置が応答可能である。

【0037】選択的に、GSMネットワーク(Global System for Mobile Communication ネットワーク)20及び車両内の電話システム18を介して、車両内の装置にアクセスする可能性がある。それにより、原則的には車両搭載ネットワークへのリモートアクセスが可能である。この場合、電話システム18は、同様に移動無線電信ネットワーク(GSMネットワーク)とその他の車両バス加入部との間のゲートウェイを意味する。

【0038】車両バス内には、車両へのアクセスを監視するカーアクセスシステム(CAS)22が組み込まれている。このCAS22は、他の機能として電子的な発進遮断部を含む。

【0039】マルチメディアチェンジャー(MMC)は、CDプレーヤと搭載ネットワークとの間のインターフェースを意味する。コントローラゲートウェイ21により、運転者が様々な器具を介して行う入力は通知情報に変換され、それぞれに応答される制御装置に転送される。

【0040】その他に、複数の制御装置(STG1～STG5)が示されている。これらの制御装置の課題は、車両内の所定のユニットの制御に限らず、これらの装置自体の間の通信にもある。ここで車両内の通信は「同報通信(ブロードキャスト)」に対応している。バスアクセスを獲得した情報発生源は、その情報を基本的に全ての制御装置に送信する。そのために、コントローラと接続されているデータバスは持続的に試問される。それ

に対して周囲環境との通信では、例えば診断バスを介して、各制御装置が一義的なアドレスを用いて的確に応答される。

【0041】制御ユニットの機能性を決定するソフトウェアは、将来的には、主にプログラミング可能なフラッシュメモリに格納される。フラッシュプログラミングでは、全ブロックだけが消去され、新たに書き込まれ得る。個々のビットの消去は不可能である。制御装置に応じて、様々な種類のマイクロコンピュータが使用される。これは、要求に応じて、8ビットプロセッサ、16ビットプロセッサ、または32ビットプロセッサである。これらの全制御装置または全コントローラは、様々なバリエーションで使用可能である。それらは、例えば、車両に搭載されているフラッシュメモリまたはプロセッサ自体に直接的に組み込まれているフラッシュメモリを有する。

【0042】次に、ここで使用される暗号方式(コード化)について詳細に説明する。使用される確認方法では、非共通暗号方式(非同期暗号方式)が有利とされる。対称鍵(共通鍵)では、各側面に秘密が所有されなくてはならない。共通鍵が知られたら、効果的な暗号化は保証され得ない。一対の鍵(鍵ペア)の1つの鍵は自動車両の制御装置内に保存される必要があり、それによりその秘密性が保証され得ないので、対称性の一対の鍵の選択は賢明ではない。

【0043】対称暗号方式(対称コード化)に対して、W.ディフィー(W.Diffie)とM.ヘルマン(M.Hellman)は1976年に所謂公開鍵暗号方式(パブリックキー暗号方式)を開発した。この暗号方式では公開鍵と秘密鍵を有する一対の鍵が形成される。公開鍵を用いて復号化は成されるが暗号化は成されない。それに対して暗号化(署名)のためには秘密鍵が必要である。

【0044】公開鍵方式は、一対の鍵の1つの鍵を公開して周知としてよいという長所を有する。しかし、今日の周知の公開鍵方式は極めて多くの計算を必要とするので、ハイブリッド方式、即ち対称方式と非対称方式の組合せが頻繁に使用されている。ハイブリッド方式では、対称鍵が公開鍵方式を用いて通信パートナー間で交換される。その際、実際の通信情報は前記対称鍵で暗号化される。

【0045】秘密鍵と公開鍵を区別することにより、確認方法並びにデジタル署名が上述したように実現される。秘密鍵を所有することにより、同一性が一義的に証明され、手書きのサインにおけるような署名が作成され得る。有名な公開鍵暗号システムは上述したRSA方式である。他の公開鍵暗号方式は、所定の数学的な群において、対数を計算するという問題に基づいている(離散対数問題)。

【0046】次に、本発明を所定の実施形態に基づいて説明する。この実施形態では、顧客が自分の車両内に所

定の追加機能を望んでいるとする。例えば、変速機が他の切替特性曲線で稼動されるべきであるとする。この機能は新たなソフトウェアを顧客の車両の制御装置内に投入することにより実現され得る。顧客は、その種のソフトウェアを提供し且つこの顧客の車両に実行可能に投入することのできる権限のある箇所、例えばディーラーに実現化を依頼する。

【0047】そのために必要なフローを次に説明する。

【0048】注文されている全ソフトウェアを唯一の箇所にてサイン（署名）させる必要をなくすために、先ずは、分散した複数の有資格者、所謂認可証所有者（例えばディーラー）が構成され、所望のソフトウェアは彼らのもとで注文され得る。認可証が授与されることにより、有資格者は、注文されたソフトウェア自体を生成し、サイン（署名）も行うことができるようになる。

【0049】このフローを先ずは図3を用いて詳細に説明する。トラストセンタ（図4における404）にて、プライベート鍵304と公開鍵302を有する第1鍵ペア（第1の一対の鍵）300が生成される。

【0050】この場合、鍵とは電子コードのことであり、この電子コードを用いて情報が暗号化及び／または復号化され得る。この際、既に上述のRSAアルゴリズムまたはDEAアルゴリズム、即ち非共通性の一対の鍵を有する所謂「公開鍵アルゴリズム（パブリックキーアルゴリズム）」のような周知の暗号アルゴリズムが使用される。

【0051】トラストセンタの公開鍵302は、車両の製造時に既に制御装置306内にてブートセクタ308に整理されている。

【0052】また、所定の認可証情報を含む認可証318は、プライベート鍵304を用いてサイン（署名）される。

【0053】同様に、認可証所有者は、他のプライベート鍵314と他の公開鍵316を有する一対の鍵312（第2鍵ペア）を提供する。公開鍵316は1つの認可証情報として認可証318内に整理される。他の認可証情報としては、例えば認可証発行者、通し番号、認可証所有者、所定のアクセス権利、有効期限などであり得る。

【0054】認可証所有者だけが知っているこの認可証所有者のプライベート鍵314を用いて、ソフトウェア320は以下に記載する方式で署名される（署名322）。次いで認可証所有者は、この認可証所有者が常に所有する認可証318、並びに提供され且つ署名されたソフトウェア320を制御装置306に投入する。

【0055】異なるプロセス方式を図6に基づいて説明する。制御装置600（図3における符号306）は、投入後のその初回の立ち上げ時に、先ず認可証618が正しいかどうかを検査する。そのために、制御装置600のブートセクタ603内に保管されているトラストセ

ンタの公開鍵602を用いて、認可証618の署名2（符号619）を検査する。認可証618がo.k.（はい）であると、認可証618内に記憶されている認可証情報617が公開鍵616と共に同様に受諾される。認可証ないしはその署名619が正しくない（いいえ）と検証されると、制御装置の稼動は停止（ストップ）される。

【0056】更に、認可証618内に含まれている公開鍵616を用いて、ソフトウェア606の署名1（符号608）がチェックされる。この検査に同様に合格（はい）すると、制御装置は、新たに投入されているソフトウェア610を用いて稼動され得る（はい）。そうでない場合（いいえ）には制御装置600の稼動は停止（ストップ）される。

【0057】説明したプロセス方式を用いると、全体として、ソフトウェアを署名するために権限が与えられている有資格箇所の分散化が達成され得る。この場合、認可証に他の資格や制限をバックするという極めて異なる可能性が開かれている。認可証内に有効期限が含まれている場合、この有効期限の経過後に、以前の認可証所有者がソフトウェアに署名することは不可能であり、ないしは、認可証が受諾されないので、このソフトウェアは受諾され得ない。更に、認可証の所有者を介して、誰が制御装置内にソフトウェアを読み込ませたか、並びにそれと共に修正を行ったかも追従することができる。

【0058】図2には他の安全レベルが示されている。車両の制御装置に新たなソフトウェアが投入されると、先ずは申告が成されなくてはならない（図2におけるステップ200）。この申告では、有資格者の識別が行われる。識別に成功すると初めて制御装置は「アンロック」され、それにより原則的には制御装置内への認可証と新たなソフトウェアの読み込みが可能となる（図2におけるステップ202）。この読み込みの後に初めて上述の認可証及びソフトウェアの検証が行われる。

【0059】次に、認可証の作成について詳細に説明する。先ず、トラストセンタと第三者との間にて、この第三者が認可証所有者として認定されて、車両の制御装置内または車両の制御装置のために変更ソフトウェアを読み込ませるという特定の資格レベルを獲得することに関して同意が交わされなくてはならない。合意が達成されると、将来的な認可証所有者（例えば修理工場400）は、プライベート鍵と公開鍵を有するこの認可証所有者固有の一対の鍵を生成し、その公開鍵を認可証要求と共にトラストセンタ404に送信する（図4におけるステップ402）。

【0060】トラストセンタ404は、認可証406を作成し、この認可証406に秘密鍵（図3における符号304も参照）を用いて署名し、この認可証406を認可証所有者400に返送し、そこでこの認可証406は保管される。

【0061】認可証所有者400は、認可証の入手以後、この認可証406が認可証所有者400に許可する範囲内で、ソフトウェア408（図3における符号320も参照）を認可証所有者400のプライベート鍵を用いて署名する。このことを図5にて説明する。そこでは、ソフトウェア500はユニット540内にて秘密鍵520を用いて署名される。それにより、署名されたソフトウェア560は車両の制御装置内に投入されるために準備が成されたことになる。このことは、図4においても示されている。そこでは、署名されたソフトウェア408並びに認可証406が認可証所有者により車両12内に投入される。

【0062】図7a～図7dを用いて、ソフトウェアの署名及び認可証の署名、並びにそれぞれの署名のチェックについて詳細に説明する。

【0063】全電子文書をその全体において署名することは非効果的である。つまり、そのためにここでは所謂ハッシュ機能が使用される。

【0064】より正確に述べると、ソフトウェア750から、周知のハッシュ機能を介して所謂ハッシュコード751が生成される。ここでハッシュコード751とは、所定の長さを有するデジタル情報に関するものである。引き続き、このハッシュコード751は認可証所有者の秘密鍵を用いて署名される（署名1（符号752））。ハッシュコード751を署名することは、長いソフトウェア文書の署名よりも基本的に効果的である。この場合、周知のハッシュ機能は次のような本質的な特徴を有する。即ち、与えられているハッシュ値 h に対して文書の値 M を見つけることは一般的に困難である（一方向機能）。更に、衝突、即ちハッシュ値が同じである2つの値 M 及び M' を見つけることは困難である（耐衝突性）。

【0065】要求されているソフトウェア753は、上述したように、認可証所有者自身により提供されて署名され得る。

【0066】ソフトウェアに対応した方式で認可証が提供される（図7b）。認可証所有者の公開鍵を含む全認可証情報760から、同様のまたは他のハッシュ機能を介して他のハッシュコード761が生成される。ここでハッシュコード761とは、他の所定の長さを有するデジタル情報に関するものである。引き続き、他のハッシュコード761はトラストセンタの秘密鍵を用いて署名される（署名2（符号762））。

【0067】新たなソフトウェア並びに認可証を制御装置に投入した後に、先ず次の稼動では、制御装置内に記憶されている公開鍵を用いて、認可証の署名が正しいかどうかがチェックされる（図7c）。そのため、制御装置からの公開鍵が署名2に適用され、ハッシュコード（符号765）が計算から得られる。この計算されたハッシュコード765が、コンパレータ764にて、認可

証自体から上記のハッシュ機能により形成されるハッシュコード761' と比較される。ここでは、両方のハッシュコード765及び761' は互いに一致しないものとしている。この場合、認可証は不当に変更されたものである。それにより、制御装置の稼動は遮断される（ストップ）。

【0068】認可証が正しいと検証されたとすると、次のステップ（図7d）では、ソフトウェアが正しく署名されたかどうかがチェックされる。そのために、対応的にソフトウェアの署名1に認可証からの公開鍵が適用され、それにより、ハッシュコード756が決定される。このハッシュコード756は、ソフトウェアから直接的に決定されるハッシュコード751' とコンパレータ754にて比較される。ここではそれらは一致していないので、更に制御装置の稼動が遮断されることになる。両方のハッシュコード756及び751' が一致するのであれば、制御装置は新たなソフトウェアを用いて稼動され得る。各立ち上げ時のチェックを回避するために、初回の検証後に検査ビットが設定され得て、この検査ビットは正しい検証を提示する。当然のことながら、この種の検査ビットは外部から修正不可能である。

【0069】上述のデジタル署名の他に、通信パートナーAを通信パートナーBに対して確認するために、所謂チャレンジレスポンス方式が頻繁に使用されている。そこでは、Bが先ず乱数RANDOMをAに送信する。Aは秘密鍵を用いて前記乱数に署名し、この値を回答としてBに送信する。Bは公開鍵を用いて前記回答を検証し、Aの確認を検査する。

【0070】次に、図8に基づいて、上述のチャレンジレスポンス方式に関する、所定の車両用のソフトウェアの個別化における保証について説明する。

【0071】上述のソフトウェアの署名方法は、制御装置ソフトウェアが所定の車両のために個別化されるよう特徴付けられるという点で拡張される。各ソフトウェアは、所定の車両の識別目印または所定の車両タイプの識別目印と関連付けられている。この識別目印は例えば車体番号である。

【0072】次に、何故、特徴付けられているソフトウェアが所定の車両ないしは所定の車両タイプにて機能可能な方式で投入され得るかを説明する。

【0073】ソフトウェアを個別化するために、先ずソフトウェア800に車体番号FGNswを登録し、引き続いてソフトウェア全体が、公開鍵IFSp804と共に、上述したようにハッシュコードの作成後に署名される（符号802）。制御装置806は既述したように正しく署名されているソフトウェアだけを受諾する。車体番号FGNswがハッシュコードと署名に影響を及ぼすので、車体番号を後で追加的に変更することは不可能である。

【0074】署名802が基本的に受諾されると、ソフ

トウェア800に割り当てられている車両識別目印FGNswが、車両内に実際に設けられている目印FGN（車体番号）と一致するかどうかがチェックされる。一致する場合にはソフトウェアが解放される。それにより、上述したように準備されているソフトウェアが所定の車両においてだけ使用され得る。更に、他の車両のためには、固有の署名を有する他のソフトウェアが提供されなくてはならない。

【0075】この種のソフトウェアの個別化を実施し得るためには、既に製造段階にて、対応する制御装置に、改ざん不能な形式で車体番号が登録されるべきである。この車体番号FGNはメモリの消去後にも制御装置内に存在しなくてはならない。このことは、車体番号が例えば上述のカーアクセスシステム（CAS）810にて非揮発性のメモリ内に登録されていることにより実現可能である。

【0076】図8による次のプロセス方式は、改ざん不可能な試問を保証する。車体番号に加えて、秘密鍵IFSsと上述の公開鍵IFSpから成る車両固有の他の一对の鍵が必要とされる。これらの2つの鍵の割り当てと車体番号の割り当ては中央箇所にて行われる。秘密鍵IFSsはカーアクセスシステム（CAS）810内に読み出し不可能な形式で記憶されている。

【0077】車体番号FGNは、カーアクセスシステムのアクセス領域に既に設けられている。

【0078】新たに投入すべきソフトウェア内には、車体番号に加えて車両固有の公開鍵IFSpも保管される（符号804）。その後、ソフトウェア800全体が署名により保護される。制御装置806内へのソフトウェアのロード後に、先ずは署名の正確性が検査される。その後、制御装置806は、既述のチャレンジレスポンスー試問を用いて、ソフトウェア内の車体番号が車両の車体番号と一致するかどうかをチェックする。そのため制御装置は、ソフトウェアからの車体番号FGNswと乱数RANDOMをカーアクセスシステム810に送信する（符号808）。カーアクセスシステム810では、車両内に記憶されている車体番号FGNが、受信された車体番号FGNswと比較される。引き続いで前記の両方の値が秘密鍵IFSsを用いて署名され、再び制御装置806に戻るように送信される。制御装置806は、署名されている送信情報を公開鍵IFSpを用いてチェックすることが可能である。その後、互いに属する異なる値が一致するかどうかが比較される（ステップ814）。一致する場合（OK）には、制御装置806は車両固有のソフトウェアを用いて稼動され得る。比較が否定的な結果を導いた場合には、制御装置の稼動はストップされる（ステップ816）。

【0079】この方法の変形例として、固有の一対の鍵IFSs及びIFSpの代わりに、車両に個別化されていない対応的な一対の鍵も使用され得て、この一対の鍵

は既に車両内に記憶されている。それにより前記の鍵用の管理が省略される。同様に、対称暗号方式を用いた対応的な機構も当然のことながら可能である。これは、処理において有利であるが、対称鍵が制御装置から読み出される危険性をもたらしてしまう。

【0080】当然のことながら、上述した全ての方法において、トラストセンタの秘密鍵が秘密であり続けるということが絶対的に保証されなくてはならない。全体的に既述の暗号手法は、正しいソフトウェアだけを車両ないしは所定の車両に投入し、それにより資格を伴わない改ざんを防止する良好な可能性を提供する。

【図面の簡単な説明】

【図1】車両における制御装置構成を示す図である。

【図2】制御装置内にソフトウェアを読み込ませるためのフローを示す図である。

【図3】ソフトウェアが正しく制御装置を制御し得るために個々の署名を授与することに関するフローを示す図である。

【図4】トラストセンタによる認可証の授与を示す図である。

【図5】ソフトウェアのためのデジタル署名の作成を示す図である。

【図6】投入されているソフトウェアを検証するための、制御装置内におけるチェックに関するフローを示す図である。

【図7】図7a～図7dは、ハッシュコードを使用した認可証とソフトウェアの暗号化及び検証を示す図である。

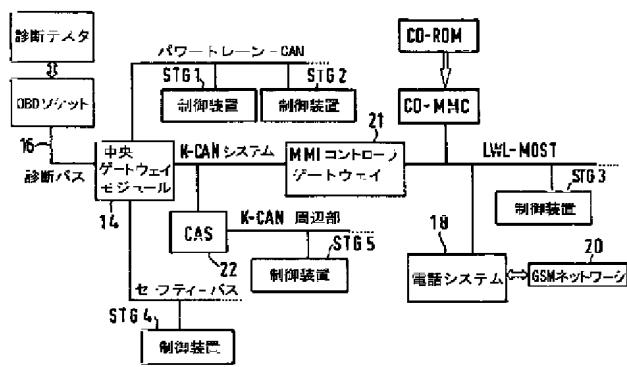
【図8】車両固有情報をチェックするためのアルゴリズムを示す図である。

【符号の説明】

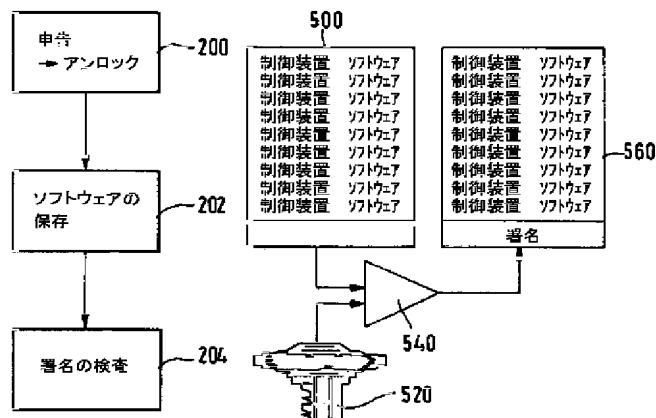
- 1 2 車両
- 1 4 中央ゲートウェイ
- 1 6 診断バス
- 1 8 電話システム
- 2 0 GSMネットワーク
- 2 1 コントローラゲートウェイ（MMI (Men Machine Interface)コントローラゲートウェイ）
- 2 2 CAS (カーアクセスシステム)
- 2 0 0 申告を行うステップ
- 2 0 2 認可証とソフトウェアの読み込みを行うステップ
- 2 0 4 認可証及びソフトウェアの検証を行うステップ
- 3 0 0 第1鍵ペア
- 3 0 2 第1鍵ペアの公開鍵（トラストセンタの公開鍵）
- 3 0 4 第1鍵ペアのプライベート鍵（秘密鍵）
- 3 0 6 制御装置
- 3 0 8 制御装置のブートセクタ

3 1 2	第2鍵ペア	7 5 0	ソフトウェア
3 1 4	第2鍵ペアのプライベート鍵（秘密鍵）	7 5 1	ソフトウェアからのハッシュコード
3 1 6	第2鍵ペアの公開鍵	7 5 1'	ソフトウェアからのハッシュコード
3 1 8	認可証	7 5 2	署名1（ソフトウェア）
3 2 0	ソフトウェア	7 5 3	署名されたソフトウェア
3 2 2	ソフトウェアの署名	7 5 4	コンパレータ
4 0 0	修理工場（認可証所有者）	7 5 6	署名1からのハッシュコード
4 0 2	認可証要求を行うステップ	7 6 0	認可証情報
4 0 4	トラストセンタ	7 6 1	認可証情報からのハッシュコード
4 0 6	認可証	7 6 1'	認可証情報からのハッシュコード
4 0 8	署名されたソフトウェア	7 6 2	署名2（認可証）
5 0 0	ソフトウェア	7 6 3	署名された認可証情報
5 2 0	秘密鍵（認可証所有者の秘密鍵）	7 6 4	コンパレータ
5 4 0	ユニット	7 6 5	署名2からのハッシュコード
5 6 0	署名されたソフトウェア	8 0 0	投入されているソフトウェア（署名済）
6 0 0	制御装置	8 0 2	署名
6 0 2	公開鍵（トラストセンタの公開鍵）	8 0 4	公開鍵
6 0 3	制御装置のブートセクタ	8 0 6	制御装置
6 0 6	ソフトウェア	8 0 8	車体番号F G N s wと乱数R A N D O Mを制御装置がC A Sへ送信するステップ
6 0 8	ソフトウェアの署名1	8 1 0	C A S（カーアクセスシステム）
6 1 0	新たに投入されたソフトウェア	8 1 2	C A Sにて署名された車体番号F G Nと乱数R A N D O MをC A Sが制御装置へ送信するステップ
6 1 6	公開鍵（認可証所有者の公開鍵）	8 1 4	制御装置がチャレンジ値を比較するステップ
6 1 7	認可証情報	8 1 6	制御装置の稼動をストップするステップ
6 1 8	認可証		
6 1 9	認可証の署名2		

〔図1〕

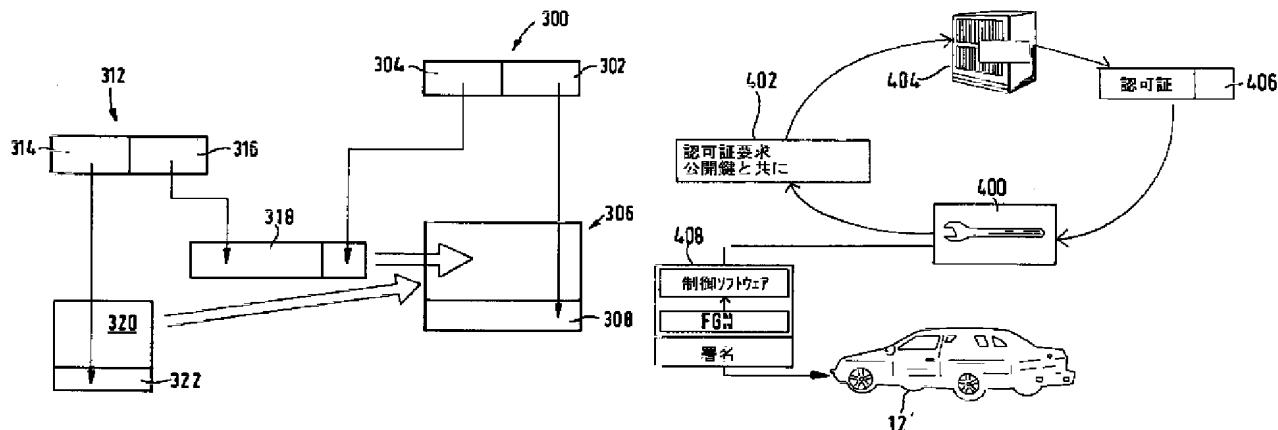


[図2]



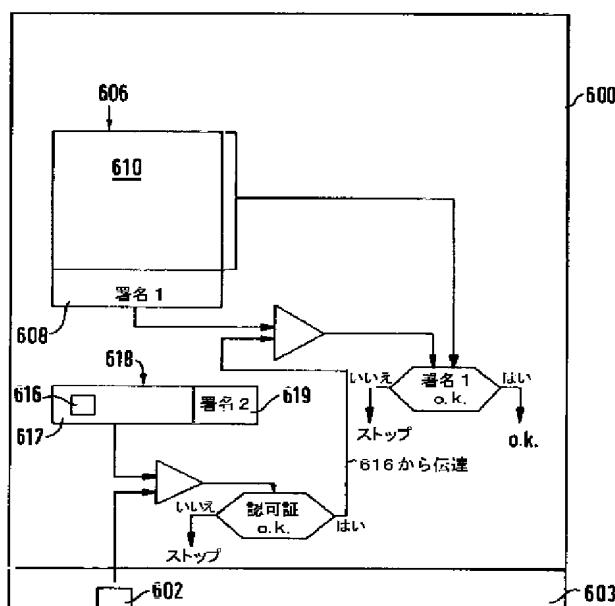
〔四〕

【図3】

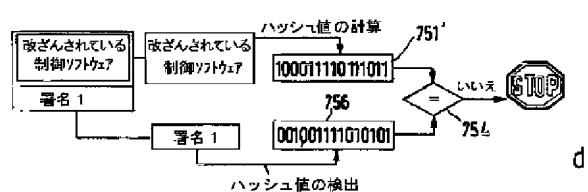
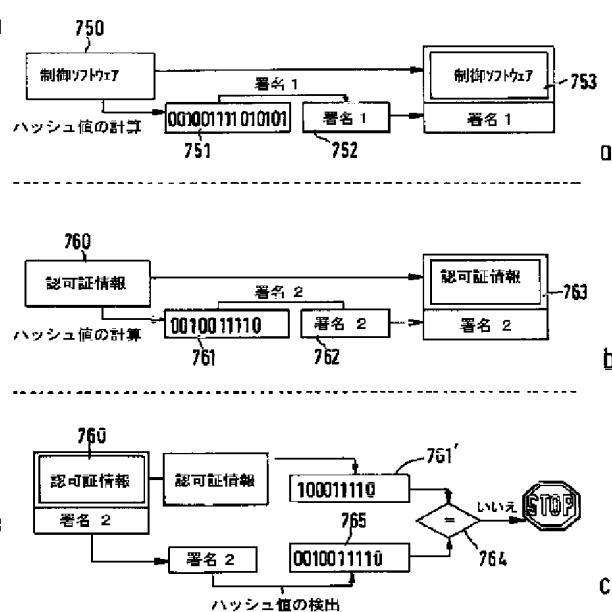


【図4】

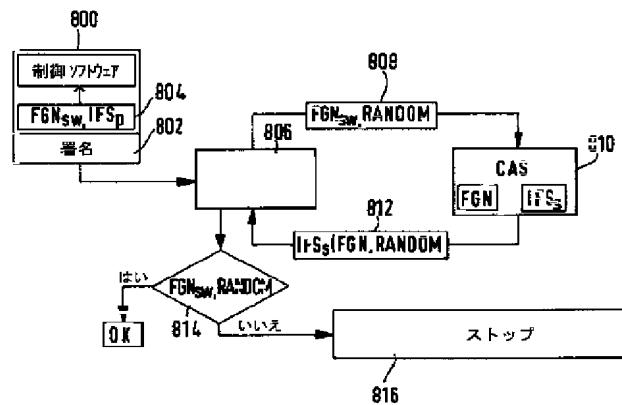
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 エルンスト シュミット
ドイツ連邦共和国 デー・85737 イスマ
ニング ベーマーヴァルトシュトラーセ
39

(72)発明者 ブルクハルト クールス
ドイツ連邦共和国 デー・81673 ミュン
ヘン ザンクト・ファイト・シュトラーセ
22